UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**SUPERSEDING**
	:	**CRIMINAL COMPLAINT**
v.	:	
	:	Honorable James B. Clark, III
MIKHAIL VASILIEV	:	
	:	Mag. No. 22-12370
	:	
	:	

I, Andrew Feiter, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

s/Andrew Feiter

Andrew Feiter
Special Agent
Federal Bureau of Investigation
Special Agent Andrew Feiter attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me telephonically
on December 1, 2022

Honorable James B. Clark, III
United States Magistrate Judge

Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers – 18 U.S.C. § 371)

From at least as early as in or around September 2019 through at least as recently as in or around October 2022, in the District of New Jersey and elsewhere, the defendant,

MIKHAIL VASILIEV,

did knowingly and intentionally conspire and agree with others to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i); and

b. to knowingly and with intent to extort from any person any money and thing of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

In violation of Title 18, United States Code, Section 371.

COUNT 2
(Intentional Damage to a Protected Computer – 18 U.S.C. § 1030(a)(5)(A))

On or about November 21, 2021, in Essex County, in the District of New Jersey, and elsewhere, the defendant,

MIKHAIL VASILIEV,

did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), and 2.

COUNT 3
(Transmitting a Demand in Relation to Damaging a Protected Computer – 18 U.S.C. § 1030(a)(7))

On or about November 21, 2022, in Essex County, in the District of New Jersey, and elsewhere, the defendant,

MIKHAIL VASILIEV,

did, knowingly and with intent to extort from persons money and other things of value, transmit in interstate and foreign commerce a communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

In violation of Title 18, United States Code, Sections 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A), and 2.

COUNT 4
(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

From at least as early as in or around September 2019 through at least as recently as in or around October 2022, in the District of New Jersey and elsewhere, the defendant,

MIKHAIL VASILIEV,

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Andrew Feiter, am a Special Agent with the Federal Bureau of Investigation (the "FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background on the LockBit Ransomware Campaign and Related Technical Matters

1. At times relevant to this Complaint:

a. Ransomware was a type of malware used by cybercriminals to encrypt data stored on a victim's computer system, leaving that data inaccessible to and unusable by the victim, and to transmit data stored on a victim system to a remote computer, or both. Following a ransomware attack, perpetrators typically demanded a ransom payment from their victims, threatening to either leave encrypted data unusable, to publish or sell stolen data if the demanded ransom was not paid, or both.

b. "LockBit" was a ransomware variant that first appeared at least as early as in or around January 2020. Between then and the present, members of the LockBit conspiracy have executed at least around 1,000 LockBit attacks against victim systems both in the United States and around the world, making at least approximately $100 million in ransom demands to victims and receiving at least as much as tens of millions of dollars in actual ransom payments. In many instances, LockBit perpetrators have posted highly confidential and sensitive data stolen from LockBit victims to a publicly available website under their ownership and control (the "LockBit Data Leak Site"). In this way, LockBit has become one of the most active and destructive ransomware variants in the world.

c. The FBI has been investigating the LockBit conspiracy since in or around March 2020.

d. This investigation has established that the LockBit variant, like other ransomware variants, operated through the "ransomware-as-a-service" model ("RaaS"). The RaaS model comprises two groups of ransomware perpetrators: developers and affiliates. The developers design the ransomware and then recruit affiliates to deploy it. The affiliates, in turn, identify vulnerable computer systems, unlawfully access those systems, and deploy on those systems the ransomware designed by the developers. When victims make ransom payments after successful ransomware attacks, the developers and the affiliates each take a share of those payments.

e. Based on training, experience, and investigation, it is widely known—including to LockBit conspiracy members themselves—that the LockBit campaign employs the RaaS model and that the LockBit conspiracy comprises numerous affiliates all seeking to deploy LockBit on victim computer systems for profit.

f. Moreover, and like other ransomware variants, this investigation has established that the LockBit variant relies on a "control panel" for its operation. In the ransomware context, a "control panel" is a software dashboard made available to an affiliate by the developers to both provide that affiliate with tools necessary for the deployment of ransomware attacks and to allow developers to monitor their affiliates' activities. The LockBit control panel allowed affiliates, among other things, to develop custom builds of the LockBit ransomware for particular victims; to communicate with LockBit victims for ransom negotiation; and to publish data stolen from LockBit victims to the LockBit Data Leak Site.

g. The LockBit perpetrators hosted much of the LockBit infrastructure, including the various LockBit control panels and the LockBit Data Leak Site, on the dark web. The "dark web" comprises Internet content that requires specialized software or configurations to access and is intended for anonymous and untraceable online communication.

h. This investigation has also established that once a new affiliate joined the LockBit conspiracy, that affiliate was given their own control panel hosted at a unique domain name on the dark web.

i. The defendant, MIKHAIL VASILIEV, was a dual national of both Russia and Canada and lived in Bradford, Ontario, Canada. As detailed below, the investigation has established that VASILIEV was a member of the LockBit conspiracy. VASILIEV used a number of monikers as part of his cybercriminal activities, including Moniker-1.

j. Cobalt Strike was a network penetration software platform. It was used legitimately by network engineers and professionals to simulate a network intrusion and assess the susceptibility of a given system to such an intrusion. It was also frequently used by cybercriminals such as VASILIEV to gain and maintain access to a victim computer system, including to prepare a victim system for the deployment of ransomware. Users controlled their deployed instances of Cobalt Strike through a collaborative user platform called a "team server."

k. More specifically, Cobalt Strike, once deployed by a cybercriminal on a victim computer system, was both designed and used by the cybercriminal to either evade detection by the system's owner entirely or otherwise appear to the owner as a benign and routine process.

The LockBit Conspiracy (Counts 1 and 4)

2. In or about August 2022, members of Canadian law enforcement executed a search of VASILIEV's home in Bradford, Ontario, Canada (the "August 2022 Search").

3. During the August 2022 Search, Canadian law enforcement discovered a file named "TARGETLIST" stored on a device in VASILIEV's home that contains a list of what appears to be either prospective or historical cybercrime victims. One victim included on that list was Victim-1, a business in Essex County, New Jersey that suffered a confirmed LockBit attack on or about November 21, 2021.

4. During the August 2022 Search, Canadian law enforcement also discovered, stored on devices in VASILIEV's home:

a. screenshots of message exchanges on the Tox end-to-end-encrypted messaging platform. Certain of these screenshots appear to capture Tox exchanges with the Tox username "LockBitSupp." "LockBitSupp" appears to be shorthand for "LockBitSupport;" both are monikers known to law enforcement to be used on multiple platforms by one or more members of the LockBit conspiracy. In these exchanges, the primary user (and presumably the user who captured the screenshots) discussed with "LockBitSupp" multiple topics related to the LockBit conspiracy, including the status of stolen data stored on the LockBit server; communications with victims; the LockBit control panel; and a particular LockBit victim in Malaysia, which suffered a confirmed LockBit attack in or around November 2021.

b. a text file with the heading "LockBit Linux/ESXi locker V: 1.1" that includes what appear to be instructions for the deployment of LockBit against a victim system.

c. source code for a program designed to encrypt data stored on a Linux-based computer system. Law enforcement has learned through this investigation that members of the LockBit conspiracy have sought at various points during the conspiracy to enable LockBit to be deployed on such systems.

d. photographs of a computer screen showing usernames and passwords for various platforms belonging to employees of a LockBit victim in Canada, which suffered a confirmed LockBit attack in or about January 2022.

5. On or about October 26, 2022, members of Canadian law enforcement executed a further search of VASILIEV's home (the "October 2022 Search"). Upon entering the home, Canadian law enforcement discovered VASILIEV sitting in the garage at a table with a laptop computer (the "VASILIEV Laptop"). Canadian law enforcement then restrained VASILIEV before he was able to lock the VASILIEV Laptop.

6. On the VASILIEV Laptop, Canadian law enforcement discovered a browser window with multiple tabs open, including a tab pointed to a site named "LockBit LOGIN" and hosted at a particular dark web domain (the "LockBit Domain"). The site displayed a login screen requesting a login and a password, along with the LockBit logo—the same LockBit logo that is consistently used elsewhere by the LockBit conspiracy, for example, on the LockBit Data Leak Site.

7. Based on training, experience, and investigation, I believe that the site hosted at the LockBit Domain was a LockBit control panel. Among other bases supporting this belief:

a. Law enforcement analyzed the memory of the device on which VASILIEV had open the browser tab pointed to the LockBit Domain. That analysis showed that that device had previously navigated to subdomains within the LockBit Domain, including "/logout", "/page#builder", "/page#builder/builder_red", "/page#chats", and "/page#stats". The fact that these subdomains of the LockBit Domain had successfully been accessed from this device in the past demonstrates that VASILIEV had working credentials for the LockBit Domain. Moreover, the phrases "builder," "chats," and "stats" all relate to functions that I know based on training, experience, and investigation to be provided by the LockBit control panel.

b. Moreover, shortly after the October 2022 Search, law enforcement attempted to navigate to the LockBit Domain and, rather than observing the same login screen found on VASILIEV's device, received a message requiring the entry of a private key to connect to that domain. The fact that VASILIEV's device displayed the login screen for the LockBit Domain demonstrates that VASILIEV had already successfully entered a private key at that preliminary authentication stage allowing him to connect to that domain.

c. I know that only members of the LockBit conspiracy—that is, LockBit developers or LockBit affiliates—would have access to any site bearing the LockBit name and logo and asking for login and password credentials, and that such a site would be a LockBit control panel. LockBit victims, for example, do not receive LockBit login and password credentials at any point.

8. On the VASILIEV Laptop, law enforcement also discovered a window actively connected to and displaying a Cobalt Strike team server. That window showed that Cobalt Strike had been deployed against multiple victim computer systems and was routinely—on the order of between seconds and minutes—exchanging transmissions with those victim systems. That window showed that the Cobalt Strike process deployed locally on those victim systems bore the name of a standard Microsoft Windows system process in order to evade detection by the owners of those systems. That window showed, finally, that at least one other user also had access to the same Cobalt Strike infrastructure.

9. During the October 2022 Search, Canadian law enforcement discovered in VASILIEV's home a seed phrase for a Bitcoin wallet address. Bitcoin is a virtual currency that allows users to make payments from, and receive payments into, Bitcoin addresses under their control. Bitcoin users, in turn, can organize and store multiple Bitcoin addresses into Bitcoin wallets, some of which employ seed phrases as a master recovery key.

10. Through investigation, law enforcement identified the Bitcoin wallet associated with the seed phrase found during the October 2022 Search ("VASILIEV Wallet-1"). Law enforcement analyzed payments to VASILIEV Wallet-1 by analyzing the Bitcoin blockchain, the publicly available ledger of all transactions conducted in Bitcoin. That analysis revealed that, on or about February 5, 2022, a Bitcoin address within the VASILIEV Wallet-1 received a payment of approximately 0.80574055 BTC. That analysis further revealed that those funds originated from a ransom payment of 2.8759 BTC made around six hours earlier by a confirmed LockBit victim to a wallet address provided by the LockBit conspirators.

<u>Victim-1 (Counts 2 and 3)</u>

11. Law enforcement has confirmed that Victim-1 suffered a LockBit attack in or around November 2021. As explained above, during the August 2022 Search, law enforcement discovered Victim-1 identified on a file named "TARGETLIST" saved on a device found in VASILIEV's home.

12. Shortly after this attack, Victim-1 discovered a ransom note left by the LockBit perpetrators on its compromised system that read, in relevant part:

> LockBit 2.0 Ransomware
>
> Your data are stolen and encrypted
> The data will be published on TOR website [hyperlinks to the LockBit data leak site] if you do not pay the ransom

> You can contact us and decrypt one file for free on these TOR sites [hyperlinks to other LockBit-maintained sites]

13. This note was saved on Victim-1's system by the LockBit perpetrators in a text file named "Restore-My-Files.txt". This investigation has revealed that LockBit attacks typically transmit ransom demands to victims in this fashion and in text files bearing this filename. Specifically, this investigation has revealed that the LockBit payload, once deployed by a perpetrator on a victim system, automatically generates the "Restore-My-Files.txt" file containing the ransom note and stores it on the victim system on a location accessible to the victim system's owner.

14. Since the October 2022 Search, law enforcement has reviewed the data that was both locally and remotely accessible to the VASILIEV Laptop at the time of its seizure. Specifically, law enforcement has reviewed the memory of a remote server to which the VASILIEV Laptop was connected at the time of its seizure (the "Remote Server Memory"). Through that review, law enforcement has discovered stored in the Remote Server Memory:

a. The following string: "LockBit_247ĸ_[Victim-1].com_20.11.21.zipC:/Users/[Moniker-1]/Documents/cp.local/LockBit_247ĸ_[Victim-1].com_20.11.21.zip". Based on my training and experience, and the facts I have learned in this investigation, I believe that this string points to a zip file that was used in furtherance of or in connection with the November 2021 LockBit attack against Victim-1. And because this zip file appears to have been saved in a location identified by Moniker-1, a VASILIEV moniker, I believe that VASILIEV had control over this file.

b. The following string: "note [Victim-1].com *". Based on my training and experience, and the facts I have learned in this investigation, I believe that this string identifies a Cobalt Strike command—in this case, a Cobalt Strike command directed to a Cobalt Strike process that had already been deployed on Victim-1's system.

Victim-2

15. Law enforcement has confirmed that Victim-2, a business in Macomb County, Michigan, suffered a LockBit attack on or about January 20, 2022. As with Victim-1, Victim-2 discovered shortly after the attack a ransom note left on its compromised system by the LockBit perpetrators. And as with Victim-1, that ransom note was named "Restore-My-Files.txt" and was substantially identical to the ransom note sent to Victim-1.

16. Law enforcement has discovered stored in the Remote Server Memory:

a. The following string: "C:\Users\[Moniker-1]\Documents\LockBit_[Victim-2]_15.01.22\Restore-My-Files.txt". Based on training, experience, and investigation, I believe that this string points to a copy of the ransom note transmitted to Victim-2 after the January 2022 LockBit attack. As explained above, the ransom notes transmitted to LockBit victims are typically named "Restore-My-Files.txt."

b. A string containing the public-facing IP address of a Victim-2 computer, as well as the email address of Victim-2's information technology manager. Based on training, experience, and investigation, I know that LockBit perpetrators often research their victims' operations and personnel to, among other things, both facilitate the deployment of ransomware ransom and inform ransom negotiations with victims.

17. During the October 2022 Search, law enforcement discovered in VASILIEV's home an additional seed phrase for a Bitcoin wallet address. As with VASILIEV Wallet-1, through investigation, law enforcement identified the Bitcoin wallet associated with this additional seed phrase ("VASILIEV Wallet-2").

18. On or about January 21, 2022, and following ransom negotiations with the LockBit perpetrators, Victim-2 made a payment of around 1.8 BTC to VASILIEV Wallet-2.